R E M A R K S

Reconsideration of this application, as amended, is respectfully requested.

THE ALLOWABLE SUBJECT MATTER

The Examiner's allowance of claims 10, 11, 15, 17 and 18, and the Examiner's indication of the allowability of the subject matter of claims 5, 6, 14 and 16 are respectfully acknowledged.

THE CLAIMS

Claim 1 has been amended to incorporate the subject matter of claim 4.

Claim 4 has been amended to be rewritten in independent form and to incorporate the subject matter of allowable claim 5, thereby placing claim 4 in condition for immediate allowance.

Allowable claim 5 has been amended to be rewritten in independent form to recite the subject matter of claim 1 (but not the subject matter of claim 4) from which claim 5 formerly depended. And it is respectfully submitted that claim 5 is now also in condition for immediate allowance since it recites a feature which (as recognized by the Examiner) is not disclosed, taught or suggested by the cited references.

Allowable claim 6 has been amended to be rewritten in independent form, thereby placing claim 6 in condition for immediate allowance.

Claim 7 has been amended to depend from amended claim 1.

Claim 8 has been amended to clarify the recitation of the mode selection unit and correct the antecedent basis problem pointed out by the Examiner.

Claim 9 has been amended to delete the phrase "or the like" so as to overcome the rejection of claims 9, 12 and 13 under 35 USC 112, second paragraph.

Allowable claim 14 has been amended to be rewritten in independent form, thereby placing claim 14 in condition for immediate allowance.

And allowable claim 16 has been amended to be rewritten in independent form, thereby placing claim 16 in condition for immediate allowance.

In addition, each of claims 1-18 have been amended to make minor grammatical improvements and/or to correct minor antecedent basis problems so as to put the claims in better form for issuance in a U.S. patent. These amendments are clerical in nature and are not related to patentability and do not narrow the scope of the claims either literally or under the doctrine of equivalent. And in this connection, it is noted that allowed claims 10, 11, 15, 17 and 18 remain in condition for allowance.

Still further, new claims 19-20, 21-22 and 23-24 have been added to recite the subject matter of claims 2-3 depending from allowable claims 4, 5 and 6, respectively, new claim 25 has been added to recite the combined subject matter of claim 1 and allowable claim 6, and new claims 26-27 have been added to recite the subject matter of claims 2-3 depending from new claim 25.

It is respectfully submitted that amended independent claims 4, 5, 6, 14 and 16 and new independent claim 25 all recite subject matter indicated to be allowable by the Examiner and that these claims, as well as each of claims 19-24 and 26-27 respectively depending from claims 4, 5, 6 and 25, are now in condition for immediate allowance along with already allowed claims 10, 11, 15, 17 and 18.

In addition, it is noted that there was no prior art rejection of claims 9, 12 and 13. Accordingly, since the rejection of these claims under 35 USC 112, second paragraph, has been overcome, it is respectfully submitted that amended claims 9, 12 and 13 are also in condition for immediate allowance.

Still further, the patentability of the remaining pending claims - namely amended claims 1-3, 7 and 8 - will be explained in detail hereinbelow.

Amended claim 1 recites a camera system for detecting an alteration of image data of image data obtained by photographing an object wherein the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer. In the paragraph bridging pages 6-7 of the Office Action the Examiner asserts (with respect to prior claims 4 and 7) that USP 5,499,294 ("Friedman") discloses this feature of the present invention. In particular, the Examiner asserts that the disclosure in Friedman of a public key (which is a unique serial number identifying a camera) can be used to identify an owner - and that the owner is interpreted to

correspond to the photographer. It is respectfully pointed out, however, that the owner of the camera is not necessarily the photographer, and that several persons may share the camera. In that case, the owner of the camera and the photographer are not identical. Accordingly, it is respectfully submitted that the disclosure in Friedman does not correspond to the feature of the present invention as recited in amended claim 1 whereby the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer - and that the system of Friedman cannot achieve the advantageous effect of the claimed present invention whereby even if several persons share the camera, because the data of each photographer is used to encrypt his or her photographed images, the photographer of each image can be accurately identified. In addition, it is noted that USP 4,848,783 ("Kiyohara et al") and USP 5,862,218 ("Steinberg") which were cited with respect to claim 8 also fail to disclose, teach or suggest this claimed feature and advantageous effect of the present invention as recited in amended claim 1.

Accordingly, it is respectfully submitted that the amended claim 1, as well as claims 2-3 and 7 depending therefrom, patentably distinguish over the cited references, taken singly or in any combination, under 35 USC 102 as well as under 35 USC 103.

Amended claim 8, moreover, recites a camera system which includes a mode selection unit for selecting at least one of an alteration monitor mode for detecting whether the image data has

correspond to the photographer. It is respectfully pointed out, however, that the owner of the camera is not necessarily the photographer, and that several persons may share the camera. In that case, the owner of the camera and the photographer are not identical. Accordingly, it is respectfully submitted that the disclosure in Friedman does not correspond to the feature of the present invention as recited in amended claim 1 whereby the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer - and that the system of Friedman cannot achieve the advantageous effect of the claimed present invention whereby even if several persons share the camera, because the data of each photographer is used to encrypt his or her photographed images, the photographer of each image can be accurately identified. In addition, it is noted that USP 4,848,783 ("Kiyohara et al") and USP 5,862,218 ("Steinberg") which were cited with respect to claim 8 also fail to disclose, teach or suggest this claimed feature and advantageous effect of the present invention as recited in amended claim 1. Accordingly, it is respectfully submitted that amended claim 1 and claims 2-3 and 7 depending therefrom patentably distinguish over the cited references, taken singly or in any combination, under 35 USC 102 as well as under 35 USC 103.

Amended claim 8, moreover, recites a camera system which includes a mode selection unit for selecting at least one of an alteration monitor mode for detecting whether the image data has

been altered, a secure mode for encrypting the image data transferred from the camera to the alteration detection unit, a digital watermark mode for embedding a digital watermark in the image data, and a normal mode for taking a photograph without a security function. By contrast, Kiyohara et al relates to an information setting apparatus for a camera, and Steinberg relates to a method and an apparatus for in-camera image marking and authentication. It is respectfully submitted, however, that none of the cited references discloses, teaches or suggests a secure mode in which the (entire) image is encrypted. In addition, it is respectfully submitted that none of the cited references discloses, teaches or suggests a mode selection unit for selecting at least one of an alteration monitor mode, a secure mode, a digital watermark mode, and a normal mode as according to the present invention as recited in amended claim 8. And it is respectfully pointed out that this feature of the present invention enables the camera system of claim 8 to support a wide variety of uses. Accordingly, it is respectfully submitted that amended claim 8 also patentably distinguish over any combination of the cited references under 35 USC 103.

CLAIM FEE

The application was originally filed with 18 claims of which 4 were independent, and the appropriate claim fee was paid for such claims. The application now contains 27 claims, of which 10 are independent. Accordingly, a claim fee in the amount

of $630.00 for the addition of 6 extra independent claims and 7 extra claims in total attached hereto. In addition, authorization is hereby given to charge any additional fees which may be determined to be required to Account No. 06-1378.

* * * * * * * * * * * * * * * * * * * *

In view of the foregoing, entry of this Amendment, allowance of the claims and the passing of this application to issue are respectfully solicited.

If the Examiner has any comments, questions, objections or recommendations, the Examiner is invited to telephone the undersigned at the telephone number given below for prompt action.

Respectfully submitted,

Douglas Holtz, Esq.
Reg. No. 33,902

Frishauf, Holtz, Goodman & Chick, P.C.
767 Third Avenue - 25th Floor
New York, New York 10017-2023
Tel. No. (212) 319-4900
Fax No. (212) 319-5101
DH:

VERSION MARKED TO SHOW CHANGES MADE

Claims 1-18 have been amended as follows:

1. (Amended) A digital evidential camera system for detecting an alteration of image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of an object, and an encryption processing unit for generating [an] alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit; and

an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key, and for detecting whether the image data has been altered based on [the] a result of the decryption;

wherein the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer.

2. (Amended) A digital evidential camera system according to claim 1,

wherein the encryption processing unit [encrypts, using the encryption key, the] also utilizes data obtained by application of a predetermined function to the image data [, thereby generating] to generate the alteration detection data.

3. (Amended) A digital evidential camera system according to claim 2,

wherein the alteration detection unit detects whether or not the image data has been altered by comparing [compares] the data obtained by application of the predetermined function to the image data with [the] data obtained by decrypting the alteration detection data using the decryption key [thereby to detect whether the image data has been altered or not].

4. (Amended) A digital evidential camera system [according to claim 1,] for detecting an alteration of image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of an object, and an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit; and

an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key, and for detecting whether the image data has been altered based on a result of the decryption;

wherein the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and [the] data for identifying a photographer; and

wherein the encryption processing unit generates first data from the image data using the encryption key, generates second data from the image data using the data for identifying the photographer, and combines the first data and the second data into the alteration detection data.

5. (Amended) A digital evidential camera system [according to claim 4,] for detecting an alteration of image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of an object, and an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit; and

an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key, and for detecting whether the image data has been altered based on a result of the decryption;

wherein the encryption processing unit generates [a] first [alteration detection] data from the image data using the encryption key, generates [a] second [alteration detection] data from the image data using [the] data for identifying the photographer, and combines the first data and the second [alteration detection] data into the alteration detection data [above mentioned].

6. (Amended) A digital evidential camera system [according to claim 4, comprising] for detecting an alteration of image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of an object, and a first encryption processing unit for generating first alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit;

an alteration detection unit for decrypting the first alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key, and for detecting whether the image data has been altered based on a result of the decryption;

a storage unit for storing [the] data for identifying [the] a photographer and the encryption key; and

a second encryption processing unit for generating [the] second alteration detection data from the data for identifying the photographer; [,]

wherein the first encryption processing unit generates the first alteration detection data based on the encryption key, the image data, and the data for identifying the photographer; and

wherein the second encryption processing unit is removably mounted on the camera.

7. (Amended) A digital evidential camera system according to claim [4] 1,

wherein the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

8. (Amended) A digital evidential camera system for detecting [the] an alteration of [the] image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of the object, and an encryption processing unit for generating [the] alteration detection data using a built-in encryption key from the image data obtained by the image pickup unit; and

an alteration detection unit for decrypting the alteration detection data generated [in] by the encryption processing unit [,] using [the] a decryption key corresponding to the encryption key, and for detecting whether the image data has been altered based on [the] a result of the decryption;

wherein the camera [, in addition to the] includes a mode selection unit for selecting at least one of an alteration monitor mode for detecting whether the image data has been altered, [has] a secure mode for encrypting the image data transferred from the camera to the alteration detection unit, a

digital watermark mode for embedding a digital watermark in the image data, and a normal mode for taking a photograph without [the] a security function [, the system further comprising a mode selection unit for selecting at least the desired one of the modes].

9. (Amended) A decryption key acquisition/registration system comprising:

a decryption key server including a decryption key storage unit for storing a unique identifier to the system and a first decryption key corresponding to a first encryption key generated as a key corresponding to the identifier, and a decryption key output unit for generating [the] alteration detection data for the first decryption key using the second encryption key and outputting the alteration detection data together with the first decryption key; and

a decryption key acquisition unit including a decryption key storage unit for storing the first decryption key acquired from the decryption key server through communication means, [or the like] and an alteration detection unit for decrypting, using a second decryption key corresponding to the second encryption key, the alteration detection data supplied from the decryption key server through the communication means [or the like] and detecting whether the first decryption key has been altered based on [the] a result of the decryption.

10. (Amended) A digital image editing system for detecting [the] an alteration of image data and editing the image data, comprising:

a filing management unit for filing and managing the image data input thereto through an image input unit;

an alteration detection unit for decrypting [a] first alteration detection data attached to the image data by use of a decryption key corresponding to a first encryption key used for generating the alteration detection data, and for comparing the first alteration detection data thus decrypted with the image data thereby to detect the alteration of the image data;

an image editing unit for processing the image data; [using various functions] and

an image file updating unit for generating second alteration detection data using a second encryption key other than the first encryption key from the [edited] image data processed by the image editing unit and [the] editing history data output by the image editing unit, and for adding the second alteration detection data to the edited image data.

11. (Amended) A digital image editing system according to claim 10,

wherein the image file updating unit is removably mounted on the digital image editing system, and has stored therein [the] information for user authentication information and the second encryption key; [,] and

wherein the second alteration detection data is generated using the second encryption key and the information for user authentication.

12. (Amended) A digital image editing system according to claim 9,

wherein the editing history data is recorded in combination with the information for user authentication.

13. (Amended) A digital image editing system according to claim 9,

wherein the image data is stored in an external medium, and the image input unit inputs the image data [stored in an] from the external storage medium [,] by connecting directly to the image filing unit or through a communication line.

14. (Amended) A digital evidential camera system [according to claim 1,] for detecting an alteration of image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of an object, and an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit; and

an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key, and for

detecting whether the image data has been altered based on a result of the decryption;

wherein the image data [is] comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets; [,] and

wherein the encryption processing unit includes a selection unit for selecting at least one image data having a desired resolution from the multiple resolution image data in order to generate the alteration detection data.

15. (Amended) A digital evidential camera system according to claim 10,

wherein the image data [is] comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets; [,] and

wherein the encryption processing unit includes a selection unit for selecting at least an image data having a desired resolution from the multiple resolution image data in order to generate the alteration detection data.

16. (Amended) A digital evidential camera system [according to claim 1,] for detecting an alteration of image data obtained by photographing an object, comprising:

a camera including an image pickup unit for picking up an image of an object, and an encryption processing unit for

generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit; and

an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key, and for detecting whether the image data has been altered based on a result of the decryption;

wherein the image data [is] comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets; [,]

wherein each of the multiple resolution image data is stored in units of a predetermined small block; [,] and

wherein the encryption processing unit generates the alteration detection data in units of the small block.

17. (Amended) A digital evidential camera system according to claim 10,

wherein the image data [is] comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets; [,]

wherein each of the multiple resolution image data is stored in units of a predetermined small block; [,] and

wherein the encryption processing unit generates the alteration detection data in units of the small block.

18. (Amended) A digital image editing system according to claim 10,

wherein at least a part of the image file updating unit is removably mounted on the digital image editing system, and has stored therein editor information and the second encryption key, and

wherein the second alteration detection data is generated using the second encryption key based on the image data, and data obtained by applying a predetermined function from the editing history data output by the image editing unit.